UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/023,043	12/17/2001	David E. McDysan	RIC01059	5663

25537 7590 07/24/2006

VERIZON
PATENT MANAGEMENT GROUP
1515 N. COURTHOUSE ROAD
SUITE 500
ARLINGTON, VA 22201-2909

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 07/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/023,043	MCDYSAN, DAVID E.	
	Examiner	Art Unit	
	Tom Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 May 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 remain for examination. The correspondence filed 5/8/06 amended claims 1-3, 7-11, 14-17, and 19-21; and added claims 22-24.

Response to Arguments

2. Applicant's arguments, filed 5/8/06, with respect to the rejection of amended claim 2 (and by extension claims 10 and 17) have been fully considered and are persuasive in part. The rejection of claims 2, 10, and 17 under 35 USC 102(b) in view of Seid has been withdrawn; however, the same arguments applied to the rejection of claims 2, 10, and 17 under 35 USC 103(a) under AAPA in view of Seid are not persuasive, as AAPA discloses that its VPN technologies, upon which the teachings of Seid can be applied, in one embodiment use a differentiated services protocol (page 4, paragraph 9), which as noted by Applicant is a specific protocol that is not mentioned by Seid (see the amendment, page 11, lines 13-14).

3. Applicant's remaining arguments filed 5/8/06 have been fully considered but they are not persuasive. Applicant argues, "*The Seid et al. system is concerned with congestion control and management on a per VPN basis, whereby congestion outside of a VPN'S logical domain does not affect the performance of the VPN (see Abstract). This is no disclosure of segregating traffic in a way that permits separate logical paths to be used to reach the same destination host. That is, the Seid et al system only segregates traffic among VPNS (inter-VPN traffic), and thus, does not disclose routing traffic to the same destination host using different logical paths.*" This is incorrect. First, it is observed that a virtual circuit, as defined by Seid, comprises a logical connection between two hosts – in the illustrated case, customer premises equipment – that belong

to a single VPN (col. 4, lines 40-60, and col. 7, lines 1-15). The virtual circuit can comprise one or more virtual paths (see Figure 3), which are logical connections between any two nodes on the network, but traffic routed through any given virtual path pertains to two hosts on the same VPN (col. 2, line 56 – col. 3, line 14). While several VPs may be multiplexed on a physical link, and several VCs many be multiplexed on a VP, nevertheless the packet switching among VPs and VCs disclosed by Seid and quoted in the previous Office Actions is done specifically to manage the traffic between hosts on a single VPN, precisely to manage traffic levels separately from extra-VPN traffic (see also col. 2, lines 49-55). There is no recitation in the Seid disclosure where a packet originating from one VC (as part of one VPN) is routed to a destination host on a different VC (as part of a different VPN), as Applicant alleges. Second, assuming arguendo that the Seid reference pertained only toward managing inter-VPN traffic, observe that Seid discloses that it was known in the art that a given node can be party to multiple VPNs (Figure 1); for example, Node A is a member of VPNs 1 and 2; however, as there is no physical link between Nodes A and B on VPN 2 (col. 2, lines 1-15), a virtual path as disclosed by Seid must be constructed over the physical links connecting Node B to Node C and then from Node A to Node C (see the PP links illustrated in Figure 1), resulting in a situation where data destined for Node A can be either from Node C on VPN 1 or Node B on VPN2, such that traffic is routed to the same destination host using different logical paths over the same physical link.

Applicant further argues, "*From [col. 8:30-40 & 51-57; and col.9: 19-22], Applicants submit that one of ordinary skill in the art would not reasonably interpret a discussion of ingress and egress ordered pairs to convey information about the source of the traffic. For example, Seid et al. describes (col.*

12: 20-24) that an ingress VP identity for the incoming frame is given by the field ivpi in the connection table. The VP concept allows the isolation of traffic of one user (or VPN) from the traffic of another user (or VPN)." Applicant is incorrect. As noted above, Seid rather clearly discloses that the invention is capable of uniquely identifying each virtual path belonging to a specific VPN (col. 10, lines 22-25), and that the means by which that invention does so is through the ingress/egress port tables disclosed in the passages quoted by Applicant above and more particularly in col. 8, lines 21-23. Seid further discloses that this arrangement allows for better management of both VPN and non-VPN traffic over the same node (see also col. 7, line 60 – col. 8, line 13). Further, Applicant's statement regarding the VP concept above supports Examiner's argument, as the ability to separate traffic belonging to a particular VPN from all other traffic, including traffic belonging to unrelated VPNs, is what has been claimed; as noted here and in previous Office Actions, Seid thus reads on the claims (see also col. 2, lines 49-55).

Claim Rejections - 35 USC § 102

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1, 3-9, 11-16, and 18-22 are rejected under 35 U.S.C. 102(b) as being anticipated by Seid et al. (U.S. Patent 5,768,271).

Referring to Claim 1:

Seid discloses a network system providing a virtual private network (VPN), said network system comprising:

one or more egress routers having connections to an access network including an access link (Figs. 1-3), wherein said one or more egress routers transmit intra-VPN traffic to a destination host belonging to the VPN from sources within the VPN within a first access network connection (e.g. elements 742-509 of Fig. 7) and all extra-VPN traffic to the destination host from sources outside the VPN within a second access network logical connections for extra-VPN traffic, separate from the first access network connection (Figure 7, particularly elements 25-39; and col. 4, lines 1-10); and

a plurality of ingress routers coupled to the one or more egress routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that denial of service attacks on said access link originating from sources outside the VPN are prevented (col. 2, line 56 – col. 3, line 15).

Referring to Claim 9:

Seid discloses a network system, comprising: an access network having an access link to a destination host belonging to a virtual private network (VPN), wherein said access network supports a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN (Figure 7, and col. 4, lines 1-10); one or more egress routers having connections to the access network, wherein said one or more egress routers transmit intra-VPN traffic to the destination host via the first logical connection and transmit all extra-VPN traffic to the destination host via the second logical connection (Fig. 3; col. 8, lines 13-57); a plurality of ingress routers coupled to the one or more egress routers for

communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (Ibid, and also col. 7, line 62 – col. 8, line 13), such that denial of service attacks on said access link originating from sources outside the VPN are prevented (col. 3, lines 10-15).

Referring to Claim 16:

Seid discloses a method of providing a virtual private network (VPN), said method comprising: in an access network including the access link, providing a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN (Figure 7, and col. 4, lines 1-10); communicating, from a plurality of ingress routers to one or more egress routers, intra-VPN and extra-VPN traffic destined for a destination host, wherein said intra-VPN traffic and said extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (col. 7, line 62 – col. 8, line 15); transmitting intra-VPN traffic from said one or more egress routers to the destination host belonging to the VPN via the first logical connection, and transmitting all extra-VPN traffic from said one or more egress boundary routers to the destination host via the second logical connection (col. 2, line 56 – col. 3, line 15), such that denial of service attacks on said access link originating from sources outside the VPN are prevented (col. 3, lines 10-15).

Referring to Claim 21:

Seid discloses a method for providing a virtual private network (VPN), the method comprising the steps of: intra-VPN traffic flowing from sources included in the VPN (Figure 7, and col. 4, lines 1-10); extra-VPN traffic flowing from sources outside the VPN (Ibid); assigning a first priority level to traffic intra-VPN traffic flowing from sources included in the VPN; assigning a second priority level to traffic extra-VPN traffic flowing from sources outside the VPN; and granting, to traffic having the first priority level at the access link, precedence of access to a destination host belonging to the VPN over traffic having the second priority level (col. 10, lines 40-65; col. 12, lines 20-30), transmitting intra-VPN traffic from said one or more egress routers to the destination host via the first logical connection, and transmitting all extra-VPN traffic from said one or more egress routers toward the destination host via the second logical connection (col. 2, line 56 – col. 3, line 15).

Referring to Claims 3 and 11:

Seid discloses the limitations of Claims 1 and 9 above. Seid further discloses a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress routers (col. 5, lines 40-60).

Referring to Claim 4:

Seid discloses the limitations of Claim 1 above. Seid further discloses further comprising the access network (Figs. 1-3).

Referring to Claims 5 and 12:

Seid discloses the limitations of Claims 4 and 9 above. Seid further discloses a customer premises equipment (CPE) edge router to the access link (col. 5, lines 40-60).

Referring to Claims 6, 13, and 18:

Seid discloses the limitations of Claims 5, 12 and 16 above. Seid further discloses said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic (Figure 4).

Referring to Claims 7, 14, and 19:

Seid discloses the limitations of Claims 1, 9 and 16 above. Seid further discloses at least one of said plurality of ingress routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic (col. 12, lines 20-30).

Referring to Claims 8, 15, and 20:

Seid discloses the limitations of Claims 1, 9 and 16 above. Seid further discloses said one or more egress routers provide a plurality of different qualities of services to said intra-VPN traffic (col. 5, line 62 – col. 6, line 4).

Referring to Claim 22:

Seid discloses a method of communicating, comprising: receiving a packet that is destined for a host within a virtual private network (col. 9, lines 4-26); determining whether the packet is originated within the virtual private network or external to the virtual private network (col. 8, lines 21-23); and forwarding the packet to the host over a first logical path or a second logical path based on the determination, wherein the first logical path is designated for traffic originating within the virtual private network and the second logical path is designated for traffic originating externally to the virtual private network (col. 2, line 49 – col. 3, line 14; col. 8, lines 5-10).

Claim Rejections - 35 USC § 103

6. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Seid.

Referring to Claim 23:

Seid discloses all the limitations of claim 22. Seid further discloses wherein the steps of receiving, determining, and forwarding the packet are performed at a customer premises router configured to process the packet (col. 5, lines 40-60; col. 8, lines 20-57) Although Seid does not explicitly mention the IP protocol or IP packets, Examiner takes Official Notice that it was well known in the art by the time the invention was made to transmit IP packets over the disclosed frame relay network hardware (see also Seid, col. 19. lines 48-57; for further reference consult the RFC 1490 reference below).

7. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant Admitted Prior Art (hereinafter, "AAPA") and further in view of Seid.

Referring to Claims 1, 9, and 16:

AAPA discloses a method of providing a virtual private network (VPN) comprising one or more egress routers having connections to an access network including the access link, wherein said one or more routers transmit intra-VPN traffic and extra-VPN traffic to the destination host belonging to the VPN (page 3, line 13 – page 5, line 20; Figures 1 and 2), and a plurality of ingress routers coupled to the one or more egress routers for communication utilizing a network-based VPN protocol (Ibid).

AAPA does not disclose wherein intra-VPN and extra-VPN traffic are separated into a first and second logical connection, nor that the logical connections are partitioned such that denial of service attacks on said access link originating from sources outside the VPN are prevented. However, Seid discloses a method for resisting denial of service attacks (i.e. network congestion, as taught by AAPA, page 5, lines 5-10) on any packet-switched network (col. 19, lines 48-57), comprising partitioning intra-VPN traffic and all extra-VPN traffic into a first and second logical connection (Figure 7, and col. 4, lines 1-10) in such a manner as to prevent denial of service attacks on said access link originating from sources outside the VPN (col. 2, line 56 – col. 3, line 15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to partition traffic between intra-VPN and extra-VPN sources as disclosed by Seid into the network disclosed by AAPA. The motivation for

doing so would be to allow a network to provide and maintain a level of service to a VPN that is unperturbed by other traffic on the network, in a manner superior to that offered by the prior art (Seid: col. 2, lines 43-46; AAPA: page 5, lines 14-20).

Referring to Claims 2, 10, and 17:

AAPA and Seid disclose the limitations of Claims 1, 9 and 16 above. AAPA further discloses wherein the at least one of the plurality of ingress routers or the at least one or more egress routers logically partitions intra-VPN traffic and extra-VPN traffic using a differentiated services protocol to mark correspondingly the intra-VPN traffic and the extra-VPN traffic (AAPA: page 4, paragraph [09]).

Referring to Claims 3 and 11:

AAPA and Seid disclose the limitations of Claims 1 and 9 above. Seid further discloses a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress routers (col. 5, lines 40-60).

Referring to Claim 4:

AAPA and Seid disclose the limitations of Claim 1 above. Seid further discloses further comprising the access network (Figs. 1-3).

Referring to Claims 5 and 12:

AAPA and Seid disclose the limitations of Claims 4 and 9 above. Seid further discloses a customer premises equipment (CPE) edge router to the access link (col. 5, lines 40-60).

Referring to Claims 6, 13, and 18:

AAPA and Seid disclose the limitations of Claims 5, 12 and 16 above. Seid further discloses said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic (Figure 4).

Referring to Claims 7, 14, and 19:

AAPA and Seid disclose the limitations of Claims 1, 9 and 16 above. Seid further discloses at least one of said plurality of ingress routers implements a plurality of tunnels that logically partition intra-VPN and extra-VPN traffic (col. 12, lines 20-30).

Referring to Claims 8, 15, and 20:

AAPA and Seid disclose the limitations of Claims 1, 9 and 16 above. Seid further discloses said one or more egress routers provide a plurality of different qualities of services to said intra-VPN traffic (col. 5, line 62 – col. 6, line 4).

Referring to Claim 21:

AAPA discloses a known prior art method for providing a virtual private network (VPN), comprising assigning a first priority level to intra-VPN traffic flowing from sources included in the VPN (page 3, lines 1-11; page 4, line 14 – page 5, line 10); assigning a second priority level to extra-VPN traffic flowing from sources outside the VPN (Ibid), and transmitting intra-VPN and extra-VPN traffic from one or more egress boundary routers to the destination host (page 3, lines 13-22; Figure 1).

It is unclear from AAPA whether the traffic having the first priority level at the access link is granted precedence of access to the destination host belonging to the VPN over traffic having the second priority level, nor that the intra-VPN and extra-VPN traffic are transmitted over a first and second logical connections, respectively. However, Seid discloses the limitations regarding the priority levels (col. 10, lines 40-65; col. 12, lines 20-30) and the first and second logical connections (col. 2, line 56 – col. 3, line 15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to partition intra-VPN and all extra-VPN traffic in the manner disclosed by Seid into the network disclosed by AAPA. The motivation for doing so would be to better prevent denial of service attacks from affecting intra-VPN traffic (col. 3, lines 10-15).

Referring to Claim 22:

AAPA discloses a method of communicating, comprising receiving a packet that is destined to a host within a virtual private network (page 2, paragraph 04), and

determining whether the packet is originated within the virtual private network or external to the virtual private network (page 3, paragraph 06).

AAPA does not disclose "forwarding the packet to the host over a first logical path or a second logical path based on the determination, wherein the first logical path is designated for traffic originating within the virtual private network and the second logical path is designated for traffic originating externally to the virtual private network". However, Seid discloses these limitations (col. 2, line 49 – col. 3, line 14). It would have been obvious to one of ordinary skill in the art at the time the invention was made to partition intra-VPN and all extra-VPN traffic in the manner disclosed by Seid into the network disclosed by AAPA. The motivation for doing so would be to better prevent denial of service attacks from affecting intra-VPN traffic (col. 3, lines 10-15).

Referring to Claim 23:

AAPA and Seid, disclose all the limitations of claim 22 above. AAPA discloses wherein the packet is an Internet Protocol (IP) packet (page 3, paragraph 06), and the steps of receiving, determining, and forwarding are performed at a customer premises router configured to process the IP packet (Ibid; see also Seid, col. 5, lines 40-60).

Referring to Claim 24:

AAPA and Seid, disclose all the limitations of claim 22 above. AAPA further discloses wherein the packet over the first logical path is marked at a higher priority that the second logical path using a differentiated services protocol (page 4, paragraph 09).

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure: "RFC 1490: Multiprotocol Interconnect over Frame Relay" illustrates that it has been very well known in the art for quite some time that the IP network protocol packet, which is inherently hardware independent, could be implemented over frame relay network hardware (page 7, "Format of Routed IP Datagram"; page 18, illustration; pages 24-25, "IP over Frame Relay"; etc.)

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
7/11/06

HOSUK SONG
PRIMARY EXAMINER